UNIVERSITY OF CALIFORNIA
SANTA CRUZ

GALOIS EXTENSIONS OF COMMUTATIVE RINGS AND HOPF GALOIS EXTENSIONS

A thesis submitted in partial satisfaction
of the requirements for the degree of

MASTER OF ARTS

in

MATHEMATICS

by

Glen Allen McDermott

December 2019

The Thesis of Glen Allen McDermott
is approved:

Professor Beren Sanders, Chair

Professor Jie Qing

Johan Steen, Ph.D.

Quentin Williams
Acting Vice Provost and Dean of Graduate Studies

Table of Contents

Abstract

Galois Extensions of Commutative Rings and Hopf Galois Extensions

By

Glen Allen McDermott

In this thesis we define the notion of a Galois extension of commutative rings, and present the analogue of the fundamental theorem of Galois theory in this setting. Following the work of Chase, Harrison, and Rosenberg, we show how the classical definition of a Galois extension of a field arises as a special case of this generalization. Furthermore, we generalize the notion of a Galois extension of commutative rings by replacing the Galois group with a Hopf algebra, leading to the notion of a Hopf Galois extension. We present the fundamental theorem in this context and show how the definition of a Galois extension of a commutative ring arises as a special case of this generalization.

Acknowledgments

I want to thank my advisor Beren Sanders for his support, friendship, and for the invaluable advice he provided during our time together. I would also like to thank Larry Green and Aaron Barnett for inspiring me to pursue higher education.

Introduction

In 1960 Auslander and Goldman introduced the notion of a Galois extension of commutative rings in [1]. In 1965 Chase, Harrison, and Rosenberg showed that the definition provided by Auslander and Goldman admitted many equivalent forms in their joint work [2]. This work was further generalized by Chase and Sweedler in 1969 to the notion of a Hopf Galois extension [4]. We first provide an exposition of the notion of a Galois extension of commutative rings and provide the fundamental theorem of Galois theory in this context. An equivalent definition of a Galois extension of commutative rings that is of central importance in this exposition is as follows: Let R, S be commutative rings, G a finite group of ring automorphisms of S such that $R = S^G$. We say S is a Galois extension of R with Galois group G if S is a separable R-algebra and the elements of G are strongly distinct. We call two ring homomorphisms $f, g\colon S \longrightarrow R$ strongly distinct if for each non-zero idempotent $e \in R$ there is an $s \in S$ such that $f(s)e \neq g(s)e$.

Auslander and Goldman defined separability of S as an R-algebra to mean

that S is projective over its enveloping algebra S^e, in other words, S is projective as an $S \otimes_R S$-module. As stated in [1], but not proved there, this allows one to obtain the classical notion of a Galois extension of fields as a special case when the rings R and S are replaced with fields. We demonstrate that this notion of separability does in fact lead to the classical notion of a Galois extension of fields. To do this we introduce the notion of a semisimple algebra and utilize the Artin-Wedderburn theorem which classifies such algebras as a product of matrix rings over division rings. Prior to this demonstration, we show that given a Galois extension S/R of commutative rings with Galois group G, there exists a one-to-one lattice inverting correspondence between separable R-subalgebras $T \subseteq S$ which are G-strong and subgroups H of G. We define G-strong to imply that the restriction of any two elements of G to T into S are either equal or strongly distinct. Moreover, we show that T/R is a Galois extension with Galois group H if and only if H is a normal subgroup of G.

We then introduce the notion of a Hopf Galois extension as presented in [4]. To do this we first introduce the notion of a bialgebra. A bialgebra A over a commutative ring R is a unital associative algebra that is also a counital coassociative coalgebra such that these two structures are compatible. We call the bialgebra A a Hopf algebra if A is equipped with a map $\lambda : A \longrightarrow A$, called the antipode.

In the Galois theory of commutative rings we consider the action of a group G

acting on S by means of R-algebra automorphisms. In this generalization of the Galois theory of commutative rings, we replace the group G with a familiar type of Hopf Algebra, a group ring RG. Analogous to the Galois theory of commutative rings, we consider an action of a group ring RG on S that gives rise to an action of G on S via R-algebra automorphisms. We then introduce the notion of a Galois extension in this context. To do this we establish preliminary concepts, that of an A-object and a Galois A-object. An A-object is a pair (S, α), where S is a commutative ring and $\alpha_S : S \longrightarrow S \otimes_R A$ is an R-algebra homomorphism such that certain compositions hold. This definition extends to the notion of a Galois A-object. Given an A-object, a Galois A-object has the additional structure of being equipped with an R-algebra isomorphism $\gamma_S : S \otimes_R S \longrightarrow S \otimes_R A$ such that $\gamma_S(x \otimes y) = (x \otimes 1)\alpha_S(y)$. After introducing the aforementioned preliminaries, we provide the fundamental theorem of Galois theory in this context. A large part of the theorem may be briefly and clearly expressed as follows: There is a one-to-one lattice inverting correspondence between admissible Hopf subalgebras of the dual of a Hopf Algebra, A^*, and certain R-subalgebras of S. Chase and Sweedler were unable to characterize the R-subalgebras of S that arise from this correspondence. We do not initiate an investigation into whether or not such a characterization of the R-subalgebras of S that arise in this correspondence have been determined. We conclude by showing that the definition of a Galois extension of a commuta-

tive ring provided by Chase, Harrison, and Rosenberg is easily obtainable from the definition of what it means to be a Galois A-object and vice versa.

Chapter 1

Galois Extensions of Commutative Rings

The most appealing rings for the theory that will be developed in this chapter are commutative rings with no idempotents other than 0 and 1, such as integral domains and fields. Since we prefer to present the theory for general commutative rings we provide the following definition.

Definition 1.1. Let S and T be commutative rings and $f, g\colon S \to T$ be homomorphisms. We say f and g are strongly distinct if for each non-zero idempotent element $t \in T$ there exists an element $s \in S$ such that $tf(s) \neq tg(s)$.

Remark 1.2. Observe that if the commutative ring S has only the trivial idempotents 0 and 1, f and g will be strongly distinct if and only if they are distinct.

Definition 1.3. Let R be a ring, A an R-algebra. The R-algebra $A^e := A \otimes_R A^\circ$, is called the enveloping algebra of A, where A° is the opposite algebra of A.

Remark 1.4. When A is a commutative R-algebra, $A = A^\circ$.

Definition 1.5. An R-algebra A is separable if A is projective as an A^e-module.

Remark 1.6. Observe that A is a left A^e-module via the action $(a \otimes b^\circ) \cdot c{=}acb$, $a \otimes b^\circ \in A \otimes_R A^\circ$, $c \in A$. Moreover, it follows that any left $A \otimes_R A^\circ$-module A can be viewed as an (A, A)-bimodule in a natural way.

Throughout this paper Definition 1.3 and Definition 1.5 will play a central role in binding the Galois theory of commutative rings with the classical Galois theory of fields in the sense that when R and A are replaced with fields, say L and K, L/K will be a finite separable extension in the classical sense.

Remark 1.7. As a consequence of Definition 1.5 and Remark 1.6, the surjective A^e-module homomorphism $\nu \colon A \otimes_R A^\circ \longrightarrow A$, $a \otimes b^\circ \mapsto ab$, admits a section, i.e., a right inverse of $A \otimes_R A^\circ$-modules given by $\sigma \colon A \to A \otimes_R A^\circ$, $a \mapsto \sum aa_i \otimes b_i^\circ$. The surjectivity of ν follows from observing that $\nu(a \otimes 1^\circ) = a$. Therefore there exists a split short exact sequence,

$$0 \longrightarrow ker(\nu) \longrightarrow A \otimes_R A^\circ \xrightarrow{\nu} A \longrightarrow 0$$

such that $\sigma\nu = id_A$. The right inverse σ, a homomorphism of (A, A)-bimodules, is completely determined by where it sends the element $1 \in A$, $p := \sigma(1) = \sum a_i \otimes b_i^\circ$.

Moreover, since σ is a homomorphism of (A, A)-bimodules it satisfies the condition $\sum aa_i \otimes b_i^\circ = \sum a_i \otimes b_i^\circ a$ for all $a \in A$. To see this notice $a\sigma(1) = \sum aa_i \otimes b_i^\circ$, and since $a\sigma(1) = \sigma(1)a = \sum a_i \otimes b_i^\circ a$, the result follows. Moreover, the condition that σ is a right inverse of ν is equivalent to the condition that there exists $a_i, b_i \in A$ such that $\sum a_i b_i = 1$. The image of $\sigma(1)$ under the map ν gives us $\nu\sigma(1)=\nu(a_i \otimes b_i^\circ)=\sum a_i b_i = 1$. Conversely, if σ is a right inverse of ν then the composition $A \xrightarrow{\sigma} A \otimes_R A^\circ \xrightarrow{\nu} A$ is the identity. Taking the image of $p := \sigma(1)$ under the map ν suffices. Observe that p satisfies

$$\begin{aligned} p^2 &= \sum_i (a_i \otimes b_i^\circ) \\ &= \sum_{i,j} (a_j \otimes b_j^\circ) \\ &= \sum_{i,j} (a_i a_j \otimes b_j b_i) \\ &= \sum_i a_i p b_i \\ &= (\sum_i a_i b_i) p = p. \end{aligned}$$

We will call such an element a separability idempotent.

Remark 1.8. We will frequently take advantage of the fact that showing an R-algebra A is separable is equivalent to constructing a separability idempotent $p \in A \otimes_R A^\circ$ such that $pa = ap$ for all $a \in A$ and the image of p under the map $\nu\colon A \otimes_R A^\circ \longrightarrow A$ is equal to 1, $\nu(p) = 1$.

Example 1.9. Let R be a commutative ring. Consider the ring of $n \times n$ matrices $M_n(R)$ and the R-algebra homomorphism given by:

$$\nu : M_n(R) \otimes_R M_n(R) \longrightarrow M_n(R)$$

$$\sum_{i,j,k,l}^{n} e_{ij} \otimes e_{kl} \mapsto \sum_{i,j,k,l}^{n} e_{ij}e_{kl},$$

where e_{st} denotes the elementary matrix with a 1 in the (s,t) component and 0 elsewhere, $s,t \in \{1,\cdots,n\}$. We show the element $p{:=}\sum_{i=1}^{n} e_{ij} \otimes e_{ji} \in M_n(R) \otimes_R M_n(R)$ is a separability idempotent. Let $e_{lk} \in M_n(R)$, and $j \in \{1,\cdots,n\}$ be fixed. It follows that

$$\nu(\sum_{i=1}^{n} e_{ij} \otimes e_{ji}) = \sum_{i=1}^{n} e_{ij}e_{ji} = \sum_{i=1}^{n} e_{ii} = I.$$

Moreover,

$$e_{lk}\sum_{i=1}^{n} e_{ij} \otimes e_{ji} = e_{lj} \otimes e_{jk} = (\sum_{i=1}^{n} e_{ij} \otimes e_{ji})e_{lk} = e_{lj} \otimes e_{jk}.$$

So $M_n(R)$ is a separable R-algebra by Remark 1.8.

We will come back to Example 1.9 later when we introduce what is called the Artin-Wedderburn Theorem.

Lemma 1.10. *Let S be a commutative separable R-algebra, and g: $S \longrightarrow R$ an R-algebra homomorphism. There exists a unique idempotent $p \in S$ such that $g(p) = 1$ and $g(s)p = sp$. Moreover, if $g_1, \ldots, g_n$ are pairwise strongly distinct R-algebra homomorphisms from S to R then the corresponding idempo-*

tents $p_1, \cdots, p_n$ *of* $g_1, \cdots, g_n$*, respectively, are pairwise orthogonal, in other words,* $g_i(p_j) = \delta_{ij}$.

Proof. By Remark 1.7 we know that the separability of S as an R-algebra is equivalent to the requirement that there exists $a_i, b_i \in S$ such that $\nu(p) = \sum_{i=1}^{n} a_i b_i = 1$ and $ap = pa$. Consider the element $e{:=}\sum_{i=1}^{n} g(a_i)b_i$. Since g is an R-algebra homomorphism it follows that,

$$g(e) = g(\sum_{i=1}^{n} g(a_i)b_i) = g(\sum_{i=1}^{n} a_i b_i) = g(1) = 1.$$

By Remark 1.7 we know $\sum_{i=1}^{n} sa_i \otimes b_i = \sum_{i=1}^{n} a_i \otimes b_i s$. To see that $g(s)e = se$ notice,

$$\nu((g \otimes 1)(\sum_{i=1}^{n} sa_i \otimes b_i)) = \sum_{i} g(sa_i)b_i = \sum_{i} g(s)g(a_i)b_i = g(s)e$$

$$\nu((g \otimes 1)(\sum_{i=1}^{n} a_i \otimes b_i s)) = \sum_{i} g(a_i)b_i s = es.$$

Notice that $e{:=}\sum_{i=1}^{n} g(a_i)b_i$ is an idempotent. Let $s = e$ in the above argument. To see that the idempotent e is unique, let e' be another idempotent element. Since $g(e') = 1$ and $g(s)e = se$ observe that

$$e = g(e')e = e'e = g(e)e' = e',$$

as desired.

We now prove that idempotents of pairwise strongly distinct R-algebra homomorphisms are pairwise orthogonal. Consider $g_i(s)g_i(p_j)$, since g is an R-algebra

homomorphism and $g_i(s)p_i = sp_i$ it follows that,

$$g_i(s)g_i(p_j) = g_i(sp_j) = g_i(g_j(s)p_j) = g_j(s)g_i(p_j).$$

Since the separable R-algebra homomorphisms are pairwise strongly distinct, we have that $g_i(p_j) = \delta_{ij}p_j$, as desired. □

Remark 1.11. For the rest of Chapter 1, unless stated otherwise, S will be a commutative ring, G a finite group of ring automorphisms of S, and $R = S^G$, the subring of S consisting of the elements left fixed by all elements of G.

Before presenting the theorem that characterizes what it will mean for S to be a Galois extension of a commutative ring R with Galois group G, we first introduce some important preliminaries. These preliminaries include the concept of a twisted group ring, $D(S, G)$, and the S-algebra GS, the set of all functions from G to S with pointwise addition and multiplication.

Remark 1.12. Let $D = D(S, G)$ denote the twisted group ring. Since G is finite, $D(S, G)$ is a free S-module with generators given by $u_{\sigma_1}, \cdots, u_{\sigma_n}$. Moreover, D possesses an R-algebra structure defined by the formula $(s_1u_{\sigma_i})(s_2u_{\sigma_j})$=$s_1\sigma_i(s_2)u_{\sigma_i\sigma_j}$ where $s_1, s_2 \in S$, $\sigma_i, \sigma_j \in G$. The identity of D is denoted by $u_{\sigma_{id}}$ and the map $x \mapsto xu_{\sigma_{id}}$ embeds S as a subring of D. Furthermore, S also has a natural structure as a D-module given by $(s_1u_{\sigma_i})x = s_1\sigma_i(x)$. The operation of S as a subring of D, on S as a D-module coincides with the multiplication in S. Therefore one

may identify $\mathrm{Hom}_D(S,S)$ with the subring of S consisting of elements left fixed by all elements of G. If R is any subring of S consisting of elements left fixed by G, we have $R \subset \mathrm{Hom}_D(S,S)$. This allows us to consider the R-algebra homomorphism of S-modules $j\colon D(S,G) \longrightarrow \mathrm{Hom}_R(S,S)$ given by $j(su_\sigma) = s\sigma(x)$. Moreover, any left D module M is an S-module on which G acts by multiplication. The notation M^G will denote the R-submodule of M invariant by the action by G, i.e., $M^G := \{m \in M | u_\sigma(m) = m, \forall \sigma \in G\}$.

Remark 1.13. Let GS denote the S-algebra of all functions from G to S. We may define the function $v_\sigma \in GS$ by $v_\sigma(\tau)=\delta_{\sigma\tau}$. Notice $GS = \bigoplus_{\sigma\in G} Sv_\sigma$ and the v_σ are pairwise orthogonal idempotents of GS whose sum is 1. Viewing $S \otimes_R S$ as an S-algebra via the first factor, we can consider the S-algebra homomorphism $h\colon S \otimes_R S \longrightarrow GS$ given by $h(s_1 \otimes s_2)(\sigma)) = s_1\sigma(s_2)$.

Definition 1.14. The trace of an element $s \in S$ is defined as $tr(s) := \sum_{\sigma\in G} \sigma(s)$.

Remark 1.15. A simple calculation shows that $tr(\cdot) \in \mathrm{Hom}_R(S,R)$. To see this let $\sigma' \in G$ and consider $\sigma'(tr(s))$, $s \in S$. We have

$$\sigma'(tr(s)) = \sigma'(\sum_{\sigma\in G} \sigma(s)) = \sum_{\sigma\in G} \sigma'\sigma(s).$$

Moreover, since the action by left multiplication on a group G by an element $\sigma' \in G$ is transitive, it follows that $\sum_{\sigma\in G} \sigma'\sigma(s) = \sum_{\sigma\in G} \sigma(s)$. Since every element of G fixes $tr(s)$ for all $s \in S$ and $R = S^G$, $tr(\cdot) : S \longrightarrow R$. Moreover, we have that

$tr(\cdot)$ is a R-algebra homomorphism since,

$$tr(rs) = \sum_{\sigma \in G} \sigma(rs) = \sum_{\sigma \in G} \sigma(r)\sigma(s) = r \sum_{\sigma \in G} \sigma(s) = rtr(s)$$

and

$$tr(s+t) = \sum_{\sigma \in G} \sigma(s+t) = \sum_{\sigma \in G} \sigma(s) + \sigma(t) = tr(s) + tr(t),$$

for all $s, t \in S$ and $r \in R$.

Remark 1.16. In the following Theorem we prove that the definition provided by Auslander-Goldman, (3), is equivalent to the definitions provided by Chase, Harrison, and Rosenberg. The proof of the theorem mirrors that in [2] with additional details added for clarity.

Theorem 1.17. *Let S be a commutative ring, and G a finite group of automorphisms of S such that $R = S^G$. Then the following are equivalent*:

1. *S is a separable R-algebra and the elements of G are pairwise strongly distinct when regarded as R-algebra homomorphisms from S to itself.*

2. *There exists elements $x_1, \cdots, x_n, y_1, \cdots, y_n \in S$ such that $\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1\sigma}$, for all $\sigma \in G$ and some $n \in \mathbb{N}$.*

3. *S is a finitely generated projective R-module and the homomorphism of S-modules $j \colon D \longrightarrow \mathrm{Hom}_R(S, S)$ given by $j(sv_\sigma)(x) = s\sigma(x)$, for all $x, s \in S$ and $\sigma \in G$, is an isomorphism.*

4. *Let M be a left D-module, which we may view as a left G-module via $\sigma(m) = u_\sigma m$. Then the R-algebra homomorphism $\omega\colon S \otimes_R M^G \longrightarrow M$ given by $\omega(s \otimes m) = sm$ is an S-module isomorphism.*

5. *The map $h\colon S \otimes_R S \longrightarrow GS$ is an S-algebra isomorphism.*

6. *Given $\sigma \in G$, $\sigma \neq 1$, and a maximal ideal $\mathfrak{m} \subset S$ there exists $s \in S$ dependent on $\mathfrak{m}$ such that $s - \sigma(s) \notin S$.*

Proof.

$(1) \Rightarrow (2)$:

Claim: Since S is a separable R-algebra, we have that $S \otimes_R S$ is a separable $S \otimes_R 1$-algebra.

Proof of claim: Since S is a projective $S \otimes_R S$-module, S is a direct summand of the free module $\bigoplus_{i \in I} S \otimes_R S$, $S \oplus Q = \bigoplus_{i \in I} S \otimes_R S$ for some S-module Q. We want to show that $S \otimes_R S$ is a direct summand of the module $(S \otimes_R S) \otimes_{S \otimes_R 1} (S \otimes_R S)$. Notice we can explicitly give an isomorphism of the $S \otimes_R S$-bimodules $(S \otimes_R S) \otimes_{S \otimes_R 1} (S \otimes_R S)$ and $S \otimes_R S \otimes_R S$,

$$\phi : (S \otimes_R S) \otimes_{S \otimes_R 1} (S \otimes_R S) \longrightarrow S \otimes_R S \otimes_R S$$

$$(a \otimes b) \otimes (c \otimes d) \longmapsto (ab \otimes c \otimes d).$$

Consider the functor $S \otimes_R \_\colon R\text{-Mod} \longrightarrow R\text{-Mod}$. Recall that functors preserve isomorphisms and tensors distribute over direct sums. As a conse-

quence we have that,

$$S \otimes_R (S \oplus Q) \simeq S \otimes_R S \oplus S \otimes_R Q = S \otimes_R \bigoplus_{i \in I} S \otimes_R S$$

$$= \bigoplus_{i \in I} S \otimes_R S \otimes_R S \simeq \bigoplus_{i \in I} S \otimes_R S \otimes_{S \otimes_R 1} S \otimes_R S.$$

Therefore $S \otimes_R S$ is a direct summand of the free $(S \otimes_R S, S \otimes_R S)$-bimodule $S \otimes_R S \otimes_{S \otimes_R 1} S \otimes_R S$. We have that $S \otimes_R S$ is a separable $S \otimes_R 1$-algebra, as desired. Now, consider the map:

$$f_\sigma \colon S \otimes_R S \longrightarrow S$$

$$(s_1 \otimes s_2) \longmapsto s_1 \sigma(s_2),$$

$\sigma \in G$. Clearly the maps f_σ are pairwise strongly distinct since the elements of G are. By Lemma 1.10 there exists a unique idempotent $p := \sum_{i=1}^{n} x_i \otimes y_i \in S \otimes_R S$ s.t. $f_\sigma(p) = \delta_{1\sigma}$. Taking $x_1, \cdots, x_n, y_1, \cdots, y_n \in S$ gives us (2).

(2) $\Rightarrow$ (3):

Let $x_1, \cdots, x_n, y_1, \cdots, y_n \in S$ such that $\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1\sigma}$ for all $\sigma \in G$. Consider the elements defined by $\psi_i(s) := tr(sy_i)$. By Remark 1.15 it follows that, $\psi_1, \cdots, \psi_n \in \mathrm{Hom}_R(S, R)$ and we have that

$$\sum_{i=1}^{n} \psi_i(s) x_i = \sum_{i=1}^{n} tr(sy_i) x_i$$

$$= \sum_{i=1}^{n} \sum_{\sigma \in G} \sigma(sy_i) x_i$$

$$= \sum_{i=1}^{n} \sum_{\sigma \in G} \sigma(s)\sigma(y_i)x_i$$
$$= \sum_{\sigma \in G} \sigma(s)\delta_{1\sigma}$$
$$= s.$$

Recall that a module P is projective as an R-module if and only if for all $a \in P$ there exists a set $\{a_i \in P | i \in I\}$ and a set $\{f_i \in \mathrm{Hom}_R(P, R) | i \in I\}$ such that $a = \sum_{i \in I} a_i f_i(a)$, where $f_i(a)$ is non-zero for finitely many i. We can conclude that S is a finitely generated projective R-module. To see that the map j is an isomorphism we will show that j is an R-algebra homomorphism, an epimorphism, and a monomorphism, respectively. Let $r \in R$, $s_1, s_2 \in S, u_{\sigma_1}, u_{\sigma_2} \in D$. We have that,

$$j(s_1 u_{\sigma_1} s_2 u_{\sigma_2})(x) = s_1\sigma_1(x)s_2\sigma_2(x) = j(s_1 u_{\sigma_1})(x) j(s_2 u_{\sigma_2})(x),$$

$$(j(r s_1 u_{\sigma_1})(x) + j(s_2 u_{\sigma_2})(x)) = r s_1\sigma_1(x) + s_2\sigma_2(x) = r j(s_1 u_{\sigma_1})(x) + j(s_2 u_{\sigma_2})(x).$$

Thus j is an R-algebra homomorphism. To see that j is an epimorphism, consider the element $\mathbf{u} \in \mathrm{Hom}_R(S, S)$ and let $\sum_{\sigma \in G} \sum_{i=1}^{n} \mathbf{u}(x_i)\sigma(y_i)u_\sigma \in D(S, G)$. Observe,

$$j(\sum_{\sigma \in G} \sum_{i=1}^{n} \mathbf{u}(x_i)\sigma(y_i)u_\sigma)$$
$$= j(\sum_{i=1}^{n} \mathbf{u}(x_i) tr(y_i) u_\sigma)$$
$$= j(\sum_{i=1}^{n} \mathbf{u}(x_i) tr(1 y_i) u_\sigma).$$

Exploiting the fact that $\mathbf{u} \in \mathrm{Hom}_R(S,S)$, $tr(1y_i) \in R$, and $\psi_i(s) := tr(sy_i)$, it follows that,

$$\begin{aligned} & j(\sum_{i=1}^{n} \mathbf{u}(x_i) tr(1y_i) u_\sigma) \\ &= j(\sum_{i=1}^{n} \mathbf{u}(x_i \psi_i(1)) u_\sigma) \\ &= j(\mathbf{u}(1) u_\sigma) \\ &= \mathbf{u}\sigma(1) \\ &= \mathbf{u}, \end{aligned}$$

as desired. To see that the map j is a monomorphism, consider the element $\mathbf{v} = \sum_{\tau \in G} s_\tau u_\tau \in D(S,G)$. Observe that,

$$\sum_{\sigma \in G} \sum_{i=1}^{n} (j(\mathbf{v}) x_i) \sigma(y_i) u_\sigma = \sum_{\tau \in G} \sum_{\sigma \in G} \sum_{i=1}^{n} s_\tau \tau(x_i) \sigma(y_i) u_\sigma.$$

Now, recall from (2) $\sum_{i=1}^{n} \tau(x_i)\sigma(y_i) = \delta_{\tau\sigma}$. Putting all this together yields,

$$\begin{aligned} & \sum_{\tau \in G} \sum_{\sigma \in G} \sum_{i=1}^{n} s_\tau \tau(x_i) \sigma(y_i) u_\sigma \\ &= \sum_{\tau \in G} \sum_{\sigma \in G} s_\tau \delta_{\tau\sigma} u_\sigma \\ &= \sum_{\tau \in G} s_\tau u_\tau \\ &= \mathbf{v}. \end{aligned}$$

Thus j is a monomorphism and hence an isomorphism, as desired.

(3) $\Rightarrow$ (4):

To prove ω is an S-module isomorphism we will construct an S-module inverse γ. We know S being a finitely generated projective R-module implies the existence of elements $x_1, \cdots, x_n \in S$ and $\phi_1, \cdots, \phi_n \in \mathrm{Hom}_R(S, S)$ such that $s = \sum_{i=1}^{n} x_i \phi_i(s)$, for all $s \in S$. Moreover, since the map j is an isomorphism, there exists $d_1, \cdots, d_n \in D(S, G)$ such that $j(d_i) = \phi_i$ for all $i \in \{1, \cdots, n\}$. Notice,

$$\begin{aligned} j(\sum_{i=1}^{n} x_i d_i)(s) &= \sum_{i=1}^{n} x_i j(d_i)(s) \\ &= \sum_{i=1}^{n} x_i \phi_i(s) \\ &= s. \end{aligned}$$

Therefore by (3) we have that $\sum_{i=1}^{n} x_i d_i = u_{\sigma_{id}} = 1$. Additionally, we have that $j(u_\sigma d_i)(s) = \sigma(j(d_i)(s)) = \sigma(\phi_i(s))$, and since every element of G fixes every element of R, $\sigma(\phi_i(s)) = \phi_i(s) = j(d_i)(s)$. It follows $u_\sigma d_i = d_i$, since j is a monomorphism. Thus, $d_i m \in M^G$, for all $m \in M$. Notice that $S \subset D$, $u_1 s = s$, for all $s \in S$, therefore we may view M as an S-module. Let $d \in D(S, G)$, $s \in S$, and $m' \in M^G$, then $(j(ds))(m') = d(sm')$. We define a map γ: $M \longrightarrow S \otimes_R M^G$ by $m \longmapsto \sum_{i=1}^{n} x_i \otimes d_i m$. Consider the image of $m \in M$ under the map $\omega\gamma$, we have that $\omega\gamma(m) = \omega(\sum_{i=1}^{n} x_i \otimes d_i m) = \sum_{i=1}^{n} x_i d_i m$ and since $\sum_{i=1}^{n} x_i d_i = 1$ it follows that $\omega\gamma(m) = m$. Conversely, consider the

image of $s \otimes m'$ under the map $\gamma\omega\colon S \otimes_R M^G \longmapsto S \otimes_R M^G$. We have $\gamma\omega(s \otimes m') = \gamma(sm') = \sum_{i=1}^{n} x_i \otimes d_i sm'$. Since $d_i s = \phi_i(s)$ and $\sum_{i=1}^{n} x_i\phi_i(s) = s$,

$$\sum_{i=1}^{n} x_i \otimes d_i sm = \sum_{i=1}^{n} x_i \otimes \phi_i(s)m'$$

$$= \sum_{i=1}^{n} x_i\phi_i(s) \otimes m'$$

$$= s \otimes m'.$$

Hence $\gamma\omega$ is the identity and ω is an S-module isomorphism, as desired.

(4) $\Rightarrow$ (5):

Given σ_1, $\sigma_2 \in G$, $\mathbf{u} \in GS$, let G act on GS by $\sigma_1(\mathbf{u})\sigma_2 = \sigma_1(\mathbf{u}(\sigma_1^{-1}\sigma_2))$. As a consequence of this action we have that $\sigma(s\mathbf{u}) = \sigma(s)\sigma(\mathbf{u})$ for all $s \in S$, and $\sigma \in G$. It follows that GS can be viewed as a $D(S, G)$ module, where $(su_\sigma)(\mathbf{u}) = \mathbf{s}\sigma(\mathbf{u})$. Let $M = GS$. If we apply $\sigma \in G$ to an element $\mathbf{u} \in M$ σ will fix this element $\mathbf{u}$ if and only if $\mathbf{u}$ is a G-homomorphism from G to S. Therefore the map $\gamma\colon S \longrightarrow M^G$ given by $\gamma(s)(\sigma) = \sigma(s)$ is an R-module isomorphism. Since the composition of R-module isomorphisms is an isomorphism, we may conclude the map $h{:=}\omega(1 \otimes \gamma){:}S \otimes_R S \longrightarrow GS$ is an S-module isomorphism, as desired.

(5) $\Rightarrow$ (1):

Define a function $\mathbf{w}_\sigma$ by $\mathbf{w}_\sigma(\tau) = \delta_{\sigma\tau}$, where the $\mathbf{w}_\sigma$ can be seen to be pairwise orthogonal idempotents of GS. Notice we can now write GS as

$GS = \sum_{\sigma \in G} \bigoplus S\mathbf{w}_\sigma$. Taking $\sigma = 1$ consider $\mathbf{w}_1$. From here, it is not too difficult to see that the GS-module $GS\mathbf{w}_1 = S\mathbf{w}_1$ is GS-projective. Since our map $h{:=}\omega(1 \otimes \gamma){:}S \otimes_R S \longrightarrow GS$ is an S-module isomorphism, we may view $S\mathbf{w}_1$ as a projective $S \otimes_R S$-module. Since $h(1 \otimes s)(\mathbf{w}_1) = h(s \otimes 1)(\mathbf{w}_1)$ we have that $S\mathbf{w}_1 \simeq S$ as $S \otimes_R S$-modules and therefore S is separable R-algebra. To see that the elements of G are pairwise strongly distinct we first define $h^{-1}(\mathbf{w}_1)$ to be $\sum_{i=1}^{n} x_i \otimes y_i$ then $x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_n \in S$ satisfy (2). Since S is projective as an $S \otimes_R S$-module we may take a separability idempotent $p \in S$ such that $\sigma(s)p = \tau(s)p$ for distinct $\sigma, \tau \in G$ and for all $s \in S$. Multiplying both sides of $1 = \sum_{i=1}^{n} x_i y_i$ by p we have,

$$\begin{aligned} p &= \sum_{i=1}^{n} x_i y_i p \\ &= \sum_{i=1}^{n} x_i \tau^{-1}\sigma(y_i)p \\ &= p\delta_{\tau^{-1}\sigma} \\ &= 0. \end{aligned}$$

Where the last equality follows since τ and σ are distinct. Thus, τ and σ are pairwise strongly distinct by Definition 1.1.

(2) $\Rightarrow$ (6):

If, for some element $1 \neq \sigma \in G$ and some maximal ideal $\mathfrak{m} \subseteq S$, $(1-\sigma)S \subseteq \mathfrak{m}$, then we would have from (2) that $\sum_{i=1}^{n} x_i(y_i - \sigma(y_i)) = 1 \in \mathfrak{m}$, $\Rightarrow\Leftarrow$.

$(6) \Rightarrow (2)$:

Since the ideal $(s - \sigma(s))$ is not contained in any $\mathfrak{m} \subset S$ for all $s \in S$ we have that $(s - \sigma(s))$ is S itself. Therefore given a $\sigma \in G$ there must exist elements $a_1, \cdots, a_n, b_1, \cdots, b_n \in S$ such that $\sum_{i=1}^{n} a_i(b_i - \sigma(b_i)) = 1$.

Define $a_{n+1} = -\sum_{i=1}^{n} a_i\sigma(b_i)$ and $b_{n+1} = 1$. It follows that

$$\sum_{i=1}^{n+1} a_i b_i = a_1 b_1 + \cdots + a_n b_n + a_{n+1} b_{n+1} =$$

$$a_1 b_1 + \cdots + a_n b_n - \sum_{i=1}^{n} a_i \sigma(b_j) b_{n+1} = \sum_{i=1}^{n} a_i(b_i - \sigma(b_i)) = 1$$

and

$$\sum_{i=1}^{n+1} a_j \sigma(b_j) = a_1\sigma(b_1) + \cdots + a_n\sigma(b_n) - \sum_{i=1}^{n} a_i\sigma(b_i)\sigma(b_{n+1}) =$$

$$a_1\sigma(b_1) + \cdots + a_n\sigma(b_n) - (a_1\sigma(b_1) + \cdots + a_n\sigma(b_n)) = 0.$$

Multiplying the a_i and the b_i established above for all non-trivial automorphisms of G, gives us our desired x_i and y_i respectively and (2) follows. $\square$

Definition 1.18. We say S is a Galois extension of R with Galois group G if any of the following conditions, and hence all of the conditions, of Theorem 1.17 are satisfied.

Remark 1.19. Recall Definition 1.1. Since the elements of G are ring homomorphisms from S to S, we may discuss whether or not the elements of G are strongly

distinct as homomorphisms from a subring T of S containing R into S. This gives rise to the following definition.

Definition 1.20. Let S be a Galois extension of R with Galois group G. A subring T of S containing R is said to be G-strong if the restrictions to T of any two elements of G are either equal or strongly distinct as maps from T into S.

Remark 1.21. Recall that the fundamental theorem of Galois theory for fields provides a bijection between intermediate fields E of a Galois extension L/F and subgroups H of the Galois group G. For the fundamental theorem of Galois theory for commutative rings, this correspondence exists between separable R-subalgebras $T \subseteq S$ which are G-strong and subgroups H of the Galois group G. Before presenting the fundamental theorem of Galois theory for commutative rings, we first prove a lemma used in the proof of the theorem. This lemma helps us conclude that when given a separable R-subalgebra $T \subseteq S$ which is G-strong, the elements of S that are left fixed by the elements of H are precisely the elements in T, in other words, $S^H = T$.

Lemma 1.22. *Let S be a Galois extension of R with Galois group G. Then there exists $c \in S$ such that $(1 - c)S = 0$.*

Proof. By Remark 1.15 $tr(\cdot) \in \mathrm{Hom_R(S, R)}$. Since the image of an ideal under a surjective homomorphism of rings is an ideal, $tr(S)$ is an ideal of R. We demonstrate below that this ideal is R itself by constructing a $c \in S$ such that $tr(c) = 1$.

Moreover, since S is a Galois extension of R by Theorem 1.17 (2) we can select $x_1, \cdots, x_n, y_1, \cdots, y_n$ such that $\sum_{i=1}^{n} x_i tr(y_i) = 1$. It follows that the ideal of S generated by $tr(S)$ is S. Since S is a finitely generated R-module, there exists an element $r \in tr(S)$ such that $(1-r)S = 0$. To see this, define an ideal of S by $\mathfrak{b}_i := (s_i, \cdots, s_n)$ and let $\mathfrak{b}_{n+1} = (0)$. We argue by means of induction on i the existence of an element r_i such that $(1-r_i)\mathfrak{b} \subset \mathfrak{b}_i$ and r_{n+1} will be the r in which we are looking for. If $i = 1$ then we can take $r_1 = 0$, $\mathfrak{b} = \mathfrak{b}_1$. Assume that $(1-r_i)\mathfrak{b} \subset \mathfrak{b}_i$ for some i. Since we have $\mathfrak{b} \subset (tr(S))\mathfrak{b}$ we may conclude that $(1-r_i)\mathfrak{b} \subset (tr(S))(1-r_i)\mathfrak{b} \subset (tr(S))\mathfrak{b}_i$ and $(1-r_i)s_i = \sum_{j=i}^{n} r_{ij}s_i$. Subtracting the $j = i$-th term from both sides we see that $(1-r_i-r_{ii})s_i \in \mathfrak{b}_{i+1}$ and hence it follows that we may take $(1-r_{i+1}) = (1-r_i)(1-r_i-r_{ii})$, as desired. Thus we have that $(1-r)S = 0$ and $r = 1$, we may conclude the existence of an element $c \in tr(S)$ such that $tr(c) = 1$. Consider the map $\phi\colon S \longrightarrow tr(cS), s \mapsto tr(cs)$. It follows that R is an R-module direct summand of S, a complement of R being the complement of the kernel of ϕ, as desired. □

The following Theorem will mirror that in [4] with additional details added for clarity.

Theorem 1.23. *Let S be a Galois extension of R with Galois group G, H a subgroup of G, and $T = S^H$. Then T is a separable G-strong R-algebra, S is a Galois extension of T with Galois group H, and H is the set of all elements of G*

leaving T pointwise fixed. Moreover, if H is a normal subgroup of G, then T is a Galois extension of R with Galois group G/H.

Proof. Since S is a Galois extension of R, we may choose $x_1, \cdots, x_n, y_1, \cdots, y_n \in S$ such that $\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1\sigma}$. This clearly will hold for all $\sigma \in H$ thus S is a Galois extension of T with Galois group H. By Theorem 1.17 (3) we have that S is a finitely generated projective T-module. In general, if A is a projective C-module and B is a projective D-module then $A \otimes_K B$ is a projective $C \otimes_K D$-module. It follows that $S \otimes_R S$ is a projective $T \otimes_R T$-module. Moreover, by Theorem 1.17 (1) we have that S is a separable R-algebra, i.e., S is a projective $S \otimes_R S$-module and hence a projective $T \otimes_R T$-module. By Lemma 1.22 we have that T is a T-module direct summand of S. It follows that T must also be a $T \otimes_R T$-module direct summand of S and hence T is $T \otimes_R T$-projective, hence separable. Now we need to show that T is G-strong. By Lemma 1.22, we may choose $c \in S$ such that $tr(c) = 1$, i.e., $\sum_{\rho \in H} \rho(c) = 1$. Moreover, choose $x_1, \cdots, x_n, y_1, \cdots, y_n \in S$ such that $\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1\sigma}$. Set $x_i' = \sum_{\rho \in H} \rho(x_i c)$, $y_i' = \sum_{\rho \in H} \rho(y_i)$, and $x_i', y_i' \in S^H = T$. We have that

$$\sum_{i=1}^{n} x_i' \sigma(y_i') = \delta_{\rho\sigma} = \begin{cases} 1 & \text{if } \sigma = \rho \text{ for some } \rho \in H \\ 0 & \text{otherwise} \end{cases}$$

since,

$$\sum_{i=1}^{n} x_i' \sigma(y_i')$$

$$= \sum_{i=1}^{n} \sum_{\rho \in H} \rho(x_i c) \sigma(\sum_{\rho \in H} \rho(y_i))$$

$$= \sum_{i=1}^{n} \sum_{\rho \in H} \rho(x_i) \rho(c) \sigma(\sum_{\rho \in H} \rho(y_i))$$

$$= \sum_{i=1}^{n} \sum_{\rho \in H} \rho(x_i) \sigma(\sum_{\rho \in H} \rho(y_i))$$

$$= \sum_{i=1}^{n} \sum_{\rho \in H} \rho(x_i) \sigma(\rho(y_i)) = \delta_{\rho\sigma}.$$

Now suppose that $\sigma, \tau \in G$ such that $\sigma|_T \neq \tau|_T$. Then we have $\tau\sigma^{-1} \notin H$ since $\tau\sigma^{-1}$ would not fix all elements of T. Let p be an idempotent contained in S. We have that $\tau(t)p = \sigma(t)p$ for all $t \in T$ and since $y_i' = \sum_{\rho \in H} \rho(y_i)$,

$$p = p \sum_{i=1}^{n} x_i' y_i'$$

$$= p \sum_{i=1}^{n} x_i' \tau^{-1} \sigma(y_i')$$

$$= 0.$$

Therefore $T = S^H$ is G-strong, as desired.

Now let $H_2 \in G$ be a subgroup of G leaving T pointwise fixed. Then clearly H_2 contains the subgroup H of G and $S^{H_2} = S^H = T$. Let n and n_2 be the cardinality of H and H_2 respectively. By Theorem 1.17 (5), we must have that $n = n_2$ and hence $H = H_2$.

Now we need to show that if H is a normal subgroup of G then T is a Galois extension of R. We have from the argument presented above that there exists $x_i', y_i' \in T$ such that the R-algebra T and the group G/H satisfy Theorem 1.17 (2). So suppose that $H \trianglelefteq G$, then $T^{G/H} = S^G = R$. Since H is precisely the elements of G leaving T pointwise fixed; we must have that G/H acts faithfully on T. □

Before stating the converse to Theorem 1.23, we again introduce a lemma that we will employ in the proof of the converse. In the classical Galois theory of fields the converse states that if L/F is a Galois extension with Galois group G and E is a subfield containing the base field, then the corresponding subgroup of G is the subgroup $H := Aut(L/E)$, i.e., the elements of G leaving E pointwise fixed.

Lemma 1.24 (See [2])**.** *Let S be a Galois extension of R with Galois group G and A any commutative R-algebra. Let G act on $A \otimes_R S$ by $\sigma(a \otimes s) = (a \otimes \sigma(s))$ for $s \in S$, $a \in A$, $\sigma \in G$. Then $A \otimes_R S$ is a Galois extension of A with Galois group G.*

Proof. By Lemma 1.22 we have that $A \otimes_R 1 \simeq A$ as R-algebras. Since S is a Galois extension of R with Galois group G we have by Theorem 1.17 (2) the existence of elements $x_1, \cdots, x_n, y_1, \cdots, y_n \in S$ such that $\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{1\sigma}$. Notice that if we take $1 \otimes x_1, \cdots, 1 \otimes x_n, 1 \otimes y_1, \cdots, 1 \otimes y_n \in A \otimes_R S$ then these elements satisfy condition (2) for $A \otimes_R S$. It suffices to show that $(A \otimes_R S)^G = A$. So let

$\mathbf{v} \in (A \otimes_R S)^G$, $c \in S$ such that $tr(c) = 1$. We have,

$$\mathbf{v} = \mathbf{v}(1 \otimes tr)(1 \otimes c) = (1 \otimes tr)(\mathbf{v}(1 \otimes c)) \in A \otimes_R R = A.$$

□

Theorem 1.25 (See [4]). *Let S be a Galois extension of R with Galois group G, and T any separable R-subalgebra of S which is G-strong. Let H be the subgroup of G leaving all elements of T pointwise fixed, then $S^H = T$.*

Proof. Notice that it will suffice to show that $S^H \subset T$ since we know $T \subset S^H$ by assumption. By Lemma 1.24 we have that $S \otimes_R S$ is a Galois extension of S with Galois group G, where S and G act on the first and second factor of $S \otimes_R S$ respectively. Moreover, we have that the map given in Theorem 1.17 (5), $h\colon S \otimes_R S \longrightarrow GS$ is an isomorphism. Therefore we may view GS as a Galois extension of S where G acts on GS by $\sigma\mathbf{v}(\tau) = \mathbf{v}(\sigma\tau)$, $\sigma, \tau \in G$ and $\mathbf{v} \in GS$. By Theorem 1.17 (3), S is a finitely generated projective R-module and we may recognize $S \otimes_R T$ with its image in $S \otimes_R S$. We show that $GS^H \subseteq h(S \otimes_R T)$. Let $(\sigma_1 H, \cdots, \sigma_r H)$ be the set of left coset representatives of the Galois group G, then $G = \cup_{i=1}^{r} \sigma_i H$. Notice we have that GS^H consists of all functions from G to S which are constant on the coset representatives $\sigma_i H$. Let $f_i\colon GS \longrightarrow S$ be the S-algebra homomorphism defined by $f_i(\mathbf{v}) := \mathbf{v}(\sigma_i)$. We need to show that the $f_1, \cdots, f_r$ are pairwise strongly distinct S-algebra homomorphisms from $h(S \otimes_R T)$

to S. Notice that if $i \neq j$ then it follows by definition that $\sigma_i\restriction_T \neq \sigma_j\restriction_T$. Let p be a non-zero idempotent element in S. Since T is G-strong there exists $t \in T$ such that,

$$f_i(h(1 \otimes t))p = \sigma_i(t)p \neq \sigma_j(t)p = f_j(h(1 \otimes t))p.$$

Therefore $f_1, \cdots, f_r$ are pairwise strongly distinct S-algebra homomorphisms. Lastly, since we have that T is R-separable it follows that $S \otimes_R T$ is S-separable and therefore $h(S \otimes_R T)$ is also S-separable. It follows from Lemma 1.10 that there exists pairwise orthogonal idempotents $p_1, \cdots, p_r \in h(S \otimes_R T)$, $f_i(x)p_i = xp_i$, for all $x \in h(S \otimes_R T)$ and $p_j(\sigma_i) = f_i(p_j) = \delta_{ij}$, for all $i, j \in \{1, \cdots, n\}$. The idempotents $p_1, \cdots, p_r$ form an S-basis of GS^H and since they are also contained in $h(S \otimes_R T)$ we must have $GS^H \subseteq h(S \otimes_R T)$. Since h is an isomorphism we can apply h^{-1} to $GS^H \subseteq h(S \otimes_R T)$ to obtain,

$$S \otimes_R S^H \subseteq (S \otimes_R S)^H \subseteq S \otimes_R T.$$

Applying the map $tr \otimes 1$ to the chain of inclusions above gives us,

$$(tr \otimes 1)(S \otimes_R S^H)(tr \otimes 1)(S \otimes_R S)^H \subseteq (tr \otimes 1)(S \otimes_R T).$$

It follows that $(R \otimes_R S)^H \subseteq R \otimes_R T$, therefore $S^H \subseteq T$, as desired. □

Chapter 2

Obtaining the Classical Notion of a Galois Extension of Fields

Definition 2.1. A module M over a ring R is said to be *semisimple* if M is a direct sum of simple submodules, i.e., submodules M_i of M such that M_i has no proper non-zero submodules, i.e., $M = \bigoplus_{i \in I} M_i$.

Definition 2.2. A projective resolution of an R-module M is an infinite exact sequence of R-modules

$$\cdots \longrightarrow P_n \longrightarrow \cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

where each P_i is a projective R-module. In shorthand, a projective resolution will be denoted by $\dot{P}$.

Remark 2.3. The minimal length amongst all finite projective resolutions of an R-module M is called its projective dimension. Throughout this chapter $pdim_R(M)$ or simply $pdim(M)$ will denote the projective dimension of M as an R-module. If the R-module M does not admit a projective resolution of finite length the projective dimension of M is said to be infinite. Moreover, notice that the projective dimension of a separable R-algebra S is equal to 0, $pdim_{S\otimes_R S}S = 0$. A projective resolution of S is given by $0 \longrightarrow P_0 = S \xrightarrow{id_S} M = S \longrightarrow 0$.

We will now show that S being projective as an $S \otimes_R S$-module implies that S is a finite extension of R by exhibiting a finite R-basis for S.

Theorem 2.4. *Let L and F be fields, L an F-vectorspace. If $pdim_{L\otimes_F L}L = 0$ then L is finitely generated as an F-vectorspace.*

Proof.

Notice that L is free since all modules over a field possess a basis. We need to show that L is finitely F-generated. Let $\{x_i\}$ be an F-basis of L. By Remark 1.7 $pdim_{L\otimes_F L}L = 0$ implies the existence of elements $\{y_i\}_{i=1}^n$ such that $\sum_{i=1}^{n} x_i y_i = 1$, $\sum_{i=1}^{n} sx_i \otimes y_i = \sum_{i=1}^{n} x_i \otimes y_i s$, for all $s \in L$. Let Y be the F-module generated by the elements $\{y_i\}_{i=1}^n$. If we rewrite the sx_i as a linear combination of the x_i notice the above equality implies that $y_i s$ can be rewritten as a linear combination of the y_i. This implies that Y is an ideal of L. It follows that $s = 1s = \sum_{i=1}^{n} x_i y_i s$, for all

$s \in L$. We can conclude that L is finitely F-generated and therefore L possess a finite F-basis, as desired. □

We now introduce a milestone in non-commutative algebra called the Artin-Wedderburn Theorem. In 1927 Emil Artin generalized a result of Joseph Wedderburn which classified semisimple algebras over a field. The Artin-Wedderburn Theorem classifies semisimple rings as a direct product of matrix rings. We omit the proof of this theorem but a proof is available in [4].

Remark 2.5. Recall that a module M is Artinian if M satisfies the descending chain condition on its poset of submodules.

Theorem 2.6. *Let K be a field and A a semisimple K-algebra. Then there exists positive integers r and $n_1, \cdots, n_r$, and division algebras $D_1, \cdots, D_r$ over K such that*

$$A \simeq M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r).$$

Moreover, the isomorphism is unique up to a permutation of the indices.

Example 2.7. Note that $M_n(D)$ is commutative if and only if $n = 1$ and D is a field. It follows that if A is a commutative semisimple K-algebra we have that A is a direct product of fields,

$$A \simeq D_1 \times \cdots \times D_r$$

with D_i a field.

Example 2.8. $A = K[x]/(f(x))$ where $f(x) \in K[x]$ is a non-constant polynomial that is a product of coprime irreducible polynomials $f_1(x), \cdots, f_r(x) \in K[x]$. Then A has decomposition of the form,

$$A \simeq M_1(K[x]/(f_1(x))) \times \cdots \times M_r(K[x]/(f_r(x))) \simeq K[x]/(f_1(x)) \times \cdots \times K[x]/(f_r(x)).$$

Notice this results in a special case of the chinese remainder theorem.

Remark 2.9. After introducing some new notation, we will provide two lemmas that will be used in the theorem that follows. This theorem will allow us to show that S being projective as an $S \otimes_R S$-module gives us separability in the classical sense when the rings S and R are replaced with fields.

Remark 2.10. Let S be an R-algebra, not necessarily commutative. We will write $pdim_{S^e} S \leq n$ to imply that the $S \otimes_R S$-projective resolution $\dot{P}$ of S has $P_i = 0$ for all $i > n$. Moreover, the notation $l.gl.dim(S)$ and $r.gl.dim(S)$ will denote the left global dimension and the right global dimension of the R-algebra S respectively. The left/right global dimension of a ring S is the supremum of the projective resolutions over all left/right S-modules, M, respectively. Interestingly enough, a left-semisimple ring is also a right-semisimple ring and vice versa. When S is semisimple the supremum of the projective resolutions of all left/right S-modules M is equal to 0, i.e., all left/right S-modules are projective. This allows one to speak of semisimple rings without ambiguity.

Lemma 2.11 (See [2]). *Let L and K be fields. Let A be a K-projective, K-algebra, and L a commutative K-algebra. Then $pdim_{A^e}(L \otimes_K A) \leq pdim_{A^e}(A)$. If further the natural mapping $\phi\colon K \longrightarrow L$ is a monomorphism onto a direct factor of L as a K-module then we have $pdim_{A^e}(L \otimes_K A) = pdim_{A^e}(A)$.*

Lemma 2.12 (See [2]). *If A is a K-algebra with K semisimple then $l.gl.dim(A) \leq pdim_{A^e}(A)$ and $r.gl.dim(A) \leq dim_{A^e}(A)$.*

Theorem 2.13 (See [2]). *Let F be a field and A an F-algebra, finite dimensional. In order that $pdim_{A^e}A = 0$ it is necessary and sufficient that A be classically separable, i.e., $L \otimes_F A$ be semisimple for all fields L containing F.*

Proof. Assume that $pdim_{A^e}A = 0$. Then by Lemma 2.11 and the fact that L is a field containing F, we have that $pdim(L \otimes_F A) = 0$. Therefore by Lemma 2.12 $L \otimes_F A$ is semisimple, and therefore A is separable. Conversely, assume A is a finite dimensional and separable. Extend scalars to an algebraic closure of F, L. Then $L \otimes_F A$ is a finite dimensional semisimple algebra over the algebraically closed field L. Therefore by Theorem 2.6 we have,

$$L \otimes_F A \simeq M_{n_1}(D_1) \times M_{n_2}(D_2) \times \cdots \times M_{n_r}(D_r).$$

Since there are no finite-dimensional division algebras over an algebraically closed field, other than the field itself, it follows that we must have

$$M_{n_1}(D_1) \times M_{n_2}(D_2) \times \cdots \times M_{n_r}(D_r) \simeq M_{n_1}(L) \times M_{n_2}(L) \times \cdots \times M_{n_r}(L).$$

As we saw in Example 1.9, constructing a separability idempotent for each $M_{n_i}(L)$ is always possible and therefore $pdim(M_{n_i}(L)) = 0$ for all i. It follows that

$$pdim(M_{n_1}(L) \times M_{n_2}(L) \times \cdots \times M_{n_r}(L)) = 0.$$

Thus, $L \otimes_F A$ is separable and by Lemma 2.11 we have that $pdim_{A^e} A = 0$. Therefore A is separable and we are done. □

Remark 2.14. Now we need to show that $L \otimes_K A$ being classically separable implies that L/K is a separable extension in the classical sense. We will carry out this argument by showing that L/K is a finite separable extension if and only if $L \otimes_K A$ is reduced, i.e., $L \otimes_K A$ contains no non-trivial nilpotent elements. It turns out $L \otimes_K A$ is reduced if and only if $L \otimes_K A$ is Artinian and possesses a trivial Jacobson radical if and only if $L \otimes_K A$ is semisimple for all field extensions L containing K. We will first demonstrate this equivalency of semisimplicity.

Lemma 2.15. *If a ring R is semisimple then $J(R) = 0$, where $J(R)$ is the Jacobson radical of the ring R. Conversely, if $J(R) = 0$ and R is Artinian then R is semisimple.*

Proof.

$\Longleftarrow$

Suppose that R is Artinian and has trivial Jacobson radical, i.e., $J(R) = \cap_{i=1}^{n} \mathfrak{m}_i = 0$ where $\mathfrak{m}_1, \cdots, \mathfrak{m}_n$ are the finitely many maximal ideals of R (note that if R had

infinitely many maximal ideals this would contradict the Artinian assumption). Consider the map $\psi\colon R \longrightarrow \bigoplus_{i=1}^{n} R/\mathfrak{m}_i$. Since $J(R) = 0$ we have that $ker(\psi) = 0$ and ψ is injective. Since the $\mathfrak{m}_i$ are maximal we have that $R/\mathfrak{m}_i$ is simple for all i. It follows that R is isomorphic to a submodule of the semisimple module $\bigoplus_{i=1}^{n} R/\mathfrak{m}_i$ and is therefore semisimple.

$\Longrightarrow$

Suppose that R is semisimple. Then there exists an isomorphism $\phi\colon R \longrightarrow \bigoplus_{i=1}^{n} A_i$ where each A_i is a simple R-module. Define $\mathfrak{m}_i := Ann(A_i)$ for all i. Then the $\mathfrak{m}_i$ are maximal ideals of R and we have that $J(R) \subseteq \cap_{i=1}^{n}\mathfrak{m}_i = 0$. Thus $J(R) = 0$, as desired. □

For our purpose, let us consider a finite dimensional commutative algebra R over a field F, we will show that if R has no non-trivial nilpotent elements, i.e., if R is reduced, then R is semisimple.

Lemma 2.16. *Let R be a finite dimensional commutative F-algebra, if R is reduced then R is semisimple.*

Proof. By definition, a finite dimensional commutative F-algebra R is a finite dimensional F-vectorspace. Therefore any descending chain of ideals will eventually terminate or this would contradict that R is a finite dimensional F-vectorspace. Since the Jacobson radical of an Artinian commutative ring R is nilpotent, by assumption we have that $J(R) = 0$, by 2.15 R is semisimple, as desired. □

Now that we have some equivalent definitions of what it means for a ring R to be semisimple, we have finally reached the part of our presentation where it is time to show that S being projective as an $S \otimes_R S$-module implies that S is separable in the classical sense when the rings are replaced with fields. We will prove this in a series of steps, starting with the following claim.

Lemma 2.17. *If L/K is a simple field extension, i.e., $K(\theta) = L$ for some $\theta \in L$, then $\overline{K} \otimes_K L$ is reduced if and only if L/K is a separable field extension.*

Proof.

$\Longleftarrow$

Since K is a simple field extension of L, $K(\theta) = L$ for some $\theta \in L$. Since L/K is separable, θ is a root of a monic separable polynomial $m(x) := a_n x^n + \cdots + a_1 x + a_0$ where m is taken to be of minimal degree and $a_1, \cdots, a_n \in K$. It follows that $L = K(\theta) = K[x]/m(x)$. Since $m(x)$ is separable let the factorization of m be $m(x) := (x - \alpha_1) \cdots (x - \alpha_n)$ over $\overline{K}$. It follows that

$$\overline{K} \otimes_K L \simeq \overline{K} \otimes_K K[x]/(x - \alpha_1) \cdots (x - \alpha_n),$$

where the $(x - \alpha_i)$ are pairwise coprime since m is separable. Therefore we have that

$$\overline{K} \otimes_K (K[x]/(x - \alpha_1) \times \cdots \times K[x]/(x - \alpha_n)) \simeq$$

$$\overline{K}[x]/(x - \alpha_1) \times \cdots \times \overline{K}[x]/(x - \alpha_n) \simeq \overline{K} \times \cdots \times \overline{K}.$$

Since a direct product of algebraically closed fields does not contain any non-trivial nilpotent elements, it follows $\overline{K} \otimes_K L$ is reduced.

$\Longrightarrow$

Conversely, suppose that L/K is not a separable extension of fields. Then we have that θ is not separable over K, i.e., the minimal polynomial for θ over $\overline{K}$ is given by $P(x) := (x-\alpha)^2 Q(x)$. Consider the map $\phi\colon \overline{K}[x] \longrightarrow \overline{K}[x]/P(x)$ and the element in $\overline{K}[x]$ given by $(x-\alpha)Q(x) \neq 0, 1$. Then $\phi((x-\alpha)Q(x))$ is a non-zero nilpotent element in $\overline{K}[x]/P(x)$, as desired. $\square$

Notice we have yet to reach our goal, by 2.13 we have to show that this is true for every field extension containing the base field K.

Lemma 2.18. *Let L/K be a finite extension. Then L/K is a separable extension if and only if $\overline{K} \otimes_K L$ is reduced.*

Proof.

$\Longleftarrow$

Follows from Lemma 2.17.

$\Longrightarrow$

If L/K is not separable then there is a $\theta \in L$ such that θ is not separable over K. Consider $K \subseteq K(\theta) \subseteq L$. Then the inclusion map $\psi\colon K(\theta) \hookrightarrow L$ induces an inclusion map given by $\lambda\colon \overline{K} \otimes_K K(\theta) \hookrightarrow \overline{K} \otimes_K L$. Since $\overline{K} \otimes_K K(\theta)$ has non-trivial nilpotent elements it follows that $\overline{K} \otimes_K L$ also has non-trivial nilpotent

elements, therefore $\overline{K} \otimes_K L$ is not reduced, as desired. $\square$

Lemma 2.19. *Let L/K be a finite field extension. L is a separable K-algebra if and only if L/K is a separable extension of fields.*

Proof. Notice by Theorem 2.13 it suffices to show the following are equivalent for a finite extension L/K:

(1) L/K is a separable extension of fields.

(2) $F \otimes_K L$ is reduced for every field extension F containing K.

$\Longleftarrow$

We have shown that $\overline{K} \otimes_K L$ is reduced implies that L/K is a separable extension of fields in Lemma 2.18, it suffices to show the other direction.

$\Longrightarrow$

We have shown that $\overline{K} \otimes_K L$ is reduced in Lemma 2.18. For an arbitrary field extension $K \subseteq F$, choose an algebraic closure $\overline{F}$. Since $K \subset F$ we can embed an algebraic closure of $\overline{K}$ into $\overline{F}$, $\lambda \colon \overline{K} \hookrightarrow \overline{F}$. As before, since L/K is a finite separable extension of fields this implies that $L = K(\theta)$ for some element $\theta \in L$ which is separable over K. Let $m(x) = a_n x^n + \cdots + a_1 x + a_0$ be the minimal polynomial for θ over K. This polynomial splits into distinct linear factors over $\overline{K}$ and since $\overline{K} \subset \overline{F}$, $m(x)$ also splits into distinct linear factors over $\overline{F}$. So we have that $\overline{F} \otimes_K L \simeq \overline{F}/m(x) \simeq \overline{F} \times \cdots \times \overline{F}$ which clearly has no non-trivial nilpotent elements, hence reduced. Since $\nu \colon F \hookrightarrow \overline{F}$ is an inclusion, $\psi \colon F \otimes_K L \hookrightarrow \overline{F} \otimes_K L$

is also an inclusion. Therefore $F \otimes_K L$ has no non-trivial nilpotent elements since $\overline{F} \otimes_K L$ has no non-trivial nilpotent elements. Thus $F \otimes_K L$ is reduced, as desired. $\square$

Remark 2.20. In the classical sense, we have a Galois extension when the extension L/K is finite, separable, and normal. We finally have successfully shown that S being a projective $S \otimes_R S$-module implies that S/R is a finite and separable extension in the classical sense when the rings S and R are replaced by fields. In this generalization, we had assumed that $S^G = R$; this implies that the extension S/R is normal. Since if S/R is a finite separable extension such that $S^G = R$, we have from the classical theory that every irreducible polynomial in $R[x]$ with a root in S splits in $S[x]$. Therefore S/R is a Galois extension, and we are done.

Chapter 3

Hopf Galois Extensions

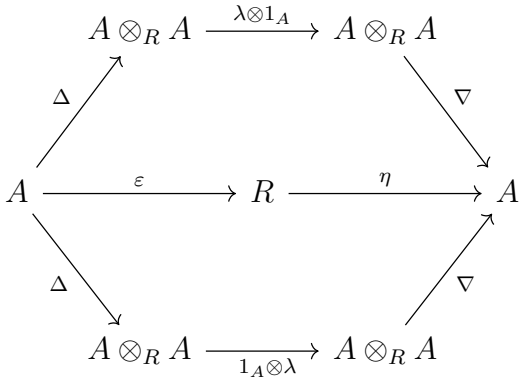
Definition 3.1. A bialgebra over a commutative ring R is an R-algebra which is both a unital associative algebra and counital coassociative coalgebra such that these structures are compatible.

Remark 3.2. Compatibility stresses that the multiplication and the unit of the algebra both be coalgebra homomorphisms, or equivalently, that the comultiplication and the counit both be algebra homomorphisms. Moreover, we will denote the algebra structure of the bialgebra by the triple (A, ∇, η) and the coalgebra stucture by the triple (A, Δ, ε). Here ∇,Δ are the multiplication and the comultiplication respectively and η,ε are the unit and counit respectively.

Definition 3.3. We call $f : A \longrightarrow B$ a bialgebra homomorphism if f is both an algebra homomorphism, and a coalgebra homomorphism.

Remark 3.4. The notion of a bialgebra can be extended to what is called a Hopf algebra if an R-linear map $\lambda : A \longrightarrow A$ can be defined as follows.

Definition 3.5. A Hopf algebra A is a bialgebra $(A, \nabla, \eta, \Delta, \varepsilon)$, over a commutative ring R equipped with a R-linear map called the antipode $\lambda\colon A \longrightarrow A$ such that the following diagram commutes:



Definition 3.6.

1. A finite Hopf algebra is a Hopf algebra A that is a finitely generated projective R-module.

2. A homomorphism of finite Hopf algebras $f\colon A \longrightarrow B$ is called a Hopf algebra homomorphism if f is a bialgebra homomorphism and f preserves antipodes, i.e., $\lambda_B f = f\lambda_A$, where $\lambda_A\colon A \longrightarrow A$ and $\lambda_B\colon B \longrightarrow B$ are the antipodes for the finite Hopf algebras A and B respectively.

3. An admissible Hopf subalgebra of a finite Hopf algebra B is the image of a surjective homomorphism $f\colon A \longrightarrow B$ of finite Hopf algebras with the following property: There exists a homomorphism $g\colon B \longrightarrow A$ of R-modules s.t. $gf = 1_A$.

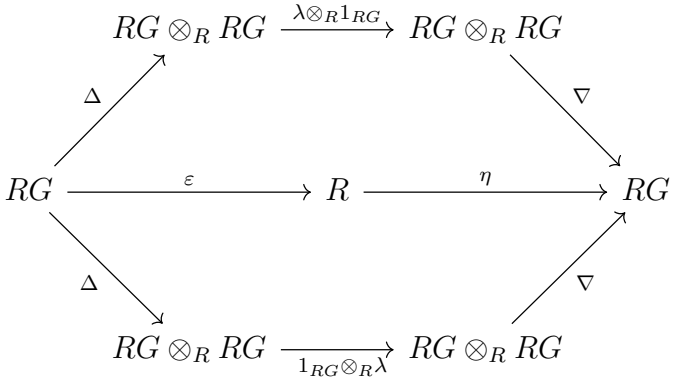
Example 3.7. A prototypical example of a finite Hopf algebra is a group ring $A = RG$, where R is a commutative ring and G is a finite group. $A = RG$ is a finite Hopf algebra via:

$$\Delta(g) = g \otimes g$$

$$\varepsilon(g) = 1_R$$

$$\lambda(g) = g^{-1}.$$

Clearly, $\lambda^2(g) = Id_{RG}$. When this is the case we say that the antipode λ is involutive. As above, we obtain the following commutative diagram:



Remark 3.8. Similar to vector spaces, if A is a finite Hopf algebra, then the dual of A, A^*, is a finite Hopf algebra as well; which is clear due to the commutativity of the diagram in Definition 3.5. Here $(-)^*$ denotes the functor $\mathrm{Hom_R}(-, \mathrm{R})$. The structure maps of A^* are given by:

$$\nabla_{A^*} \colon A^* \otimes_R A^* \longrightarrow A^*, (f \otimes g) \mapsto \mu_R \circ (f \otimes g) \circ \Delta_A$$

$$\Delta_{A^*} \colon A^* \longrightarrow A^* \otimes_R A^*, (f) \mapsto \phi(f \circ \nabla_A)$$

$$\eta_{A^*} \colon R \longrightarrow A^*, r \mapsto r\varepsilon_A$$

$$\varepsilon_{A^*} \colon A^* \longrightarrow R, (f) \mapsto f \circ \eta_A(1).$$

Where

$$\phi \colon (A \otimes_R A)^* \longrightarrow A^* \otimes_R A^*$$

$$\mu \colon R \otimes_R R \longrightarrow R$$

are both isomorphisms.

Remark 3.9. Let A be a finite Hopf algebra. Using the tensor-hom adjunction notice we have the following:

$$(A \otimes_R A)^* = \mathrm{Hom}_R(A \otimes_R A, R) \simeq \mathrm{Hom}_R(A, \mathrm{Hom}_R(A, R))$$

$$\simeq \mathrm{Hom}_R(A, R) \otimes_R \mathrm{Hom}_R(A, R) = A^* \otimes_R A^*.$$

Remark 3.10. We introduce a notation known as Sweedler notation. Let C be a coalgebra over R and $\Delta \colon C \longrightarrow C \otimes_R C$ be the comultiplication. For $c \in C$ we have that $\Delta(c) = \sum_{i=1}^{n} c_{(1)_i} \otimes c_{(2)_i}$. Due to the coassociativity of the coalgebra C and the commutative diagrams associated with C, Moss Sweedler recommended we use sumless notation for easy bookkeeping. The above sum becomes $\sum c_{(1)} \otimes c_{(2)}$,

where one can drop the $\sum$ symbol if remaining mindful that the element $c_{(1)} \otimes c_{(2)}$ could potentially be a sum of elements. Moreover, due to the coassociativity we have $\sum \Delta(c_{(1)}) \otimes c_{(2)} = \sum c_{(1)} \otimes \Delta(c_{(2)})$ which becomes

$$\sum c_{(1)(1)} \otimes c_{(1)(2)} \otimes c_{(2)} = \sum c_{(1)} \otimes c_{(2)(1)} \otimes c_{(2)(2)}.$$

Sweedler notation allows us to write this sum simply as $\sum c_{(1)} \otimes c_{(2)} \otimes c_{(3)}$. We will continue to use this notation throughout the rest of the paper.

Definition 3.11. Let A be a Hopf algebra over R. An *A-object* is a pair (S, α), where S is a commutative R-algebra and $\alpha \colon S \longrightarrow S \otimes_R A$, $x \mapsto \sum x_{(1)} \otimes x_{(2)}$ is a R-algebra homomorphism such that the maps $(\alpha \otimes 1)\alpha$ and $(1 \otimes \Delta)\alpha$ from $S \longrightarrow S \otimes_R A \otimes_R A$ are equal. Moreover the map $(1 \otimes \varepsilon)\alpha$ from S to S is the identity on S. Where $(\alpha \otimes 1)\alpha$ and $(1 \otimes \Delta)\alpha$, $x \mapsto \sum x_{(1)} \otimes x_{(2)} \otimes x_{(3)}$.

Remark 3.12. Note that one has to keep track of which algebra the $x_{(1)}, x_{(2)}, x_{(3)}$ are elements of. In the example above we have that $x_{(1)} \in S, x_{(2)}, x_{(3)} \in A$.

Remark 3.13. Recall that by Definition 3.6 a finite Hopf algebra A is a finitely generated projective R-module. By the fact that A is a finitely generated projective R-module and by the well-known tensor-hom adjunction we have the following isomorphisms $\mathrm{Hom}_R(S, S \otimes_R A) \simeq \mathrm{Hom}_R(S, \mathrm{Hom}_R(A^*, S)) \simeq \mathrm{Hom}_R(A^* \otimes_R S, S)$, respectively. Note that if S is an A-object we may apply these isomorphisms to an element $\alpha_S \in \mathrm{Hom}_R(S, S \otimes_R A)$ to obtain a map $\beta_S \colon A^* \otimes_R S \longrightarrow S$,

where $\beta_S(u \otimes x) = u(x)$. This allows us to view S as an A^*-module. Moreover, since we have two modules over the same underlying ring R, it follows that we can consider the triple $(\langle \cdot, \cdot \rangle, A, A^*)$ consisting of the two modules A and A^* and a non-degenerate R-bilinear map $\langle \cdot, \cdot \rangle \colon A^* \otimes_R A \longrightarrow R$, called the dual pair of A and A^*. From all of this follows that $u(x) = \sum x_{(1)} \langle u, x_{(2)} \rangle$ where $x \in S$ and $u \in A^*$. Additionally, since we have that $\beta_S(u \otimes 1) = \varepsilon_{A^*}(u)(1)$ and $\beta_S(u \otimes xy) = \sum_{(u)} \beta_S(u_{(1)} \otimes x) \beta_S(u_{(2)} \otimes y)$, $u \in A^*$, $x, y \in S$, we say that β_S measures S to S.

Example 3.14. When a group G is finite, we can define the dual of the group algebra RG as the set of functions with pointwise addition and multiplication from G to R, i.e., $GR = RG^* = \mathrm{Hom}_R(G, R)$. This forms a dual pair $(\langle \cdot, \cdot \rangle, RG, GR)$ as in Remark 3.13. If $x = \sum_{g \in G} a_g g$ is an element in RG and $f \colon G \longrightarrow R$ is an element of $RG^* = \mathrm{Hom}_R(G, R)$ we may define the R-bilinear map as $\langle x, f \rangle \colon = \sum_{g \in G} a_g f(g)$.

Definition 3.15. Let A be a Hopf algebra, and S be an A-object. We define the R-algebra homormorphism

$$\gamma_S \colon S \otimes_R S \longrightarrow S \otimes_R A$$

$$\gamma_S(x \otimes y) = (x \otimes 1)\alpha_S(y) = \sum xy_{(1)} \otimes y_{(2)}.$$

We will call S a Galois A-object if the following condition holds:

1. $\gamma_S \colon S \otimes_R S \longrightarrow S \otimes_R A$ is an isomorphism.

Remark 3.16. Note that when the Hopf algebra A is the Hopf algebra GR the map given in Definition 3.15 (1) becomes $\gamma_S \colon S \otimes_R S \longrightarrow S \otimes_R GR \simeq GS$, which is precisely the map given in Theorem 1.17 (5). It is this fact that allows us to conclude that S/R is a Galois extension of commutative rings with Galois group G if and only if S is a Galois GR-object.

Definition 3.17. Let A be a Hopf algebra, $\varepsilon \colon A \longrightarrow R$, the counit of A. We call the ideal $I_A = ker(\varepsilon_A)$ the augmentation ideal of A.

The following definition will be needed in the presentation of the analogue of the fundamental theorem of Galois theory of commutative rings.

Definition 3.18. Let A be a finite Hopf algebra, and S be a Galois A-object. Let B^* be an admissible Hopf subalgebra of A^*, and T a subalgebra of S. The symbol $T \to B^*$ will imply that the following condition holds: Given $w \in S \otimes_R A^*$, $w(T) = 0$ if and only if $w \in S \otimes_R A^* I_{B^*}$. Where if $w = s_1 \otimes u_1 + \cdots + s_n \otimes u_n \in S \otimes_R A^*$ and $x \in S$ we have that $w(x) = s_1 u_1(x) + \cdots + s_n u_n(x) \in S$.

Before proving the claim in Remark 3.16, we first present the Hopf analogue of the fundamental theorem of Galois theory of commutative rings; since this will be used to help us prove the claim. The following Theorem will be provided without proof but a proof is available in [4].

Theorem 3.19. *Let A be a finite commutative Hopf algebra, and S a Galois A-object. Then:*

1. *S is a finitely generated faithful projective R-module, and $S^{A^*} = R$.*

2. *If B^* is an admissible Hopf subalgebra of A^* and T is a subalgebra of S which is an R-module direct summand of S, then $T \to B^*$ if and only if $T = S^{B^*}$. If these conditions hold, then the T-algebra S is a Galois $T \otimes_R B$-object.*

3. *If $T_i \to B_i^*$ for $i \in \{1, 2\}$ where T_i,B_i^* as in (2), then $T_1 \subseteq T_2$ if and only if $B_2^* \subseteq B_1^*$. In particular, $T_1 = T_2$ if and only if $B_1^* = B_2^*$.*

4. *If B_i^* is an admissible Hopf subalgebra of A^*, then $B_1^* \subseteq B_2^*$ if and only if $S^{B_2^*} \subseteq S^{B_1^*}$.*

Now we can prove that S is a GR-object if and only if S/R is a Galois extension of commutative rings with Galois group G.

Theorem 3.20. *S is a Galois GR-object if and only if S/R is a Galois extension of commutative rings with Galois group G.*

Proof. First suppose that S is a GR-object. By Defininition 3.15 we have that the map $h = \gamma_S \colon S \otimes_R S \longrightarrow S \otimes_R GR \simeq GS$ is an S-algebra isomorphism. This map is precisely the map given in Theorem 1.17 (5). By Theorem 3.19 (1) we have that $S^G = R$. Therefore S/R is a Galois extension of commutative rings with Galois

group G. Conversely, suppose that S/R is a Galois extension of commutative rings with Galois group G. Then we have by Theorem 1.17 (5) that the map $h\colon S \otimes_R S \longrightarrow GS$ is an S-algebra isomorphism. It follows from Definition 3.15 that S is a Galois GR-object and by Theorem 3.19 (1) $S^{RG} = R$, as desired. $\square$

Bibliography

[1] Maurice Auslander and Oscar Goldman. The Brauer group of a commutative ring. *Trans. Amer. Math. Soc.*, 97:367–409, 1960.

[2] Henri Cartan and Samuel Eilenberg. *Homological algebra*. Princeton Landmarks in Mathematics. Princeton University Press, Princeton, NJ, 1999. With an appendix by David A. Buchsbaum, Reprint of the 1956 original.

[3] S. U. Chase, D. K. Harrison, and Alex Rosenberg. Galois theory and Galois cohomology of commutative rings. *Mem. Amer. Math. Soc. No.*, 52:15–33, 1965.

[4] Stephen U. Chase and Moss E. Sweedler. *Hopf algebras and Galois theory*. Lecture Notes in Mathematics, Vol. 97. Springer-Verlag, Berlin-New York, 1969.

[5] Karin Erdmann and Thorsten Holm. *Algebras and representation theory*. Springer Undergraduate Mathematics Series. Springer, Cham, 2018.

[6] Moss E. Sweedler. The Hopf algebra of an algebra applied to field theory. *J. Algebra*, 8:262–276, 1968.